

OPTIMAL CURVES OF GENUS 3 OVER FINITE FIELDS WITH DISCRIMINANT -19

E. ALEKSEENKO, S. ALESHNIKOV, N. MARKIN, A. ZAYTSEV

ABSTRACT. In this work we study the properties of maximal and minimal curves of genus 3 over finite fields with discriminant -19 . We prove that any such curve can be given by an explicit equation of certain form (see Theorem 5.1). Using these equations we obtain a table of maximal and minimal curves over finite fields with discriminant -19 of cardinality up to 997. We also show that existence of a maximal curve implies that there is no minimal curve and vice versa.

1. INTRODUCTION

The number of rational points of an irreducible non-singular projective curve C/\mathbb{F}_q of genus g satisfy the Hasse-Weil-Serre bound:

$$|\#C(\mathbb{F}_q) - q - 1| \leq g[2\sqrt{q}].$$

In case of equality, i.e. the number of rational points of the curve is $q + 1 + g[2\sqrt{q}]$ (resp. $q + 1 - g[2\sqrt{q}]$), then the curve is called *maximal over \mathbb{F}_q* (resp. *minimal over \mathbb{F}_q*). We will call such curves *optimal over \mathbb{F}_q* .

Let C be an optimal curve of genus g over \mathbb{F}_q . Then the Frobenius endomorphism induces a homomorphism

$$F : T_l \text{Jac}(C) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow T_l \text{Jac}(C) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where $T_l \text{Jac}(C)$ is the projective limit $\varprojlim \text{Jac}(C)[l^n]$. Moreover, if the characteristic polynomial of $\text{Jac}(C)$ splits

$$P_{\text{Jac}(C)}(T) = \prod_{i=1}^{2g} (T - \alpha_i),$$

then the number of rational points on C equals to

$$\#C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^g \alpha_i = q + 1 - \sum_{i=1}^g (\alpha_i + \bar{\alpha}_i),$$

The research the fourth authors was supported by the Claude Shannon Institute, Science Foundation Ireland Grant 07/RFP/ENM123.

with $\alpha_{i+g} = \bar{\alpha}_i$. The eigenvalues of the endomorphism Frobenius F have following property: $\alpha_i + \bar{\alpha}_i = -[2\sqrt{q}]$ when C is maximal and $\alpha_i + \bar{\alpha}_i = [2\sqrt{q}]$ when C is minimal. Therefore, if a curve is optimal, then the L -polynomial of this curve is determined by

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t) = \prod_{i=1}^g (1 \mp [2\sqrt{q}]t + qt^2)$$

for minimal (resp. maximal) case. Then the theory of Honda-Tate shows that the Jacobian $\text{Jac}(C)$ of a maximal (resp. minimal) curve C is isogenous to a product of copies of a maximal (resp. minimal) elliptic curve, i.e. $\text{Jac}(C) \sim E^g$, where E is a maximal (resp. minimal) elliptic curve over a finite field \mathbb{F}_q . The isogeny class of E over a finite field \mathbb{F}_q is characterized by the characteristic polynomial of the Frobenius endomorphism of E .

We consider the equivalence between the category of ordinary abelian varieties $\text{Jac}(C)$ over \mathbb{F}_q which are isogenous to E^g (hence E is ordinary) and the category of R -modules, where R is the ring defined by the Frobenius endomorphism of E . In our case let C be a smooth irreducible projective algebraic curve over a finite field \mathbb{F}_q with discriminant -19 . Therefore $R = \mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-19})$. Let $\text{Jac}(C)$ be the principal polarized Jacobian variety of C with Theta-divisor θ . By Torelli's Theorem, the curve C is completely defined by $(\text{Jac}(C), \theta)$, up to a unique isomorphism over an algebraic closure of \mathbb{F}_q . Consider the Hermitian module $(\mathcal{O}_K^g; h)$, where \mathcal{O}_K^g is a \mathcal{O}_K -module, and $h : \mathcal{O}_K^g \times \mathcal{O}_K^g \rightarrow \mathcal{O}_K$ is a Hermitian form. The equivalence of categories is defined by the functor $\mathcal{F} : \text{Jac}(C) \rightarrow \text{Hom}(E, \text{Jac}(C))$ and its inverse $\mathcal{V} : \mathcal{O}_K^g \rightarrow \mathcal{O}_K^g \otimes_{\mathcal{O}_K} E$. Under this equivalence the principal polarisation of Jacobian $\text{Jac}(C)$ corresponds to an irreducible Hermitian \mathcal{O}_K -form h . Therefore we can use the classification of unimodular irreducible Hermitian forms in order to study the isomorphism classes of $\text{Jac}(C)$. For a detailed description of this equivalence of categories see the Appendix by J.-P. Serre in [3].

Deligne's Theorem [1] yields that the number of isomorphism classes of abelian varieties isogenous to A equals the number of isomorphism classes of R -modules, which may be embedded as lattices in the K -vector space K^g , where $K = \text{Quot}(R)$. Since in our case there exists one isomorphism class of such R -modules, then there exists a unique isomorphism class of abelian varieties. Therefore Deligne's Theorem together with 2.1 show that $\text{Jac}(C)$ is actually isomorphic to E^g .

The main result of this paper is putting this theory to practical use. We give a characterization of isomorphism classes of optimal curves of

genus 3 over finite fields with discriminant -19 in such a way that we are able to give an explicit description of all such curves. In particular, we produce maximal and minimal curves of genus 3 over finite fields with discriminant -19 of cardinality up to 997.

2. OPTIMAL CURVES OF GENUS 1 AND 2

2.1. Optimal Elliptic Curves. In this subsection we explore optimal elliptic curves over \mathbb{F}_q and produce concrete calculations for the finite fields \mathbb{F}_q of the discriminant -19 and $q \leq 1000$.

The endomorphism ring $\text{End}(E)$ of an elliptic curve E is the set of all isogenies $\phi : E(\overline{\mathbb{F}}_q) \rightarrow E(\overline{\mathbb{F}}_q)$, with multiplication corresponding to composition. If a curve E has complex multiplication, then by Deuring's theory [7] the endomorphism ring $\text{End}(E)$ is an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$. The theory of complex multiplication and Deuring's lifting theory give us the following: given a quadratic field K , the number of isomorphism classes of elliptic curves over \mathbb{F}_q whose endomorphism rings are isomorphic to the maximal order \mathcal{O}_K is equal to the number of ideal classes h_K of K .

Proposition 2.1. *Let \mathbb{F}_q be a finite field with discriminant -19 . There exist exactly two \mathbb{F}_q -isomorphism classes of optimal elliptic curves E over \mathbb{F}_q , namely the class of maximal and the class of minimal elliptic curves over \mathbb{F}_q .*

Proof. Deuring's Theorem provides the existence of maximal and minimal elliptic curves over a finite field with discriminant -19 . Let E be such a curve. Then $\text{End}_{\mathbb{F}_q}(E)$ contains the ring $\mathbb{Z}[x]/(x^2 + mx + q)$, where $m = \pm[2\sqrt{q}]$ is the trace of the Frobenius endomorphism of E . Therefore we have $\text{End}_{\mathbb{F}_q}(E) \cong \mathcal{O}_K \cong \mathbb{Z}[x]/(x^2 + mx + q)$, where K is the imaginary quadratic field $\mathbb{Q}(\sqrt{-19})$ with discriminant -19 . We have $\mathcal{O}_K = \mathbb{Z}[\frac{-19+\sqrt{-19}}{2}]$ and Minkowski's bound is $B_K \approx 2,77$. Then any non-principal ideal class must be representable by an ideal of norm $\leq 2,77$. We verify that $2\mathcal{O}_K$ is a principal ideal to conclude that $h_K = 1$. From the class number and the mass formula (see [6]) it follows that there exists a unique class of isomorphic elliptic curves over \mathbb{F}_q . \square

Remark 2.2. Alternatively, we can find the number of \mathbb{F}_q -isomorphism classes of elliptic curves over \mathbb{F}_q within a given isogeny class by using the following properties. If two elliptic curves are given by $E : y^2 = x^3 + ax + b$ and $E' : y^2 = x^3 + a'x + b'$, then $E \cong E'$ over \mathbb{F}_q if and only if the following relations on the coefficients hold: $a' = ac^4, b' = bc^6$ for a some $c \in \mathbb{F}_q$.

Example 2.3. We give examples of maximal and minimal elliptic curves over finite fields over \mathbb{F}_q with discriminant -19 for all $q < 1000$.

q	Maximal	Minimal
47	$y^2 = x^3 + x + 38$	$y^2 = x^3 + 32x + 27$
61	$y^2 = x^3 + 6x + 29$	$y^2 = x^3 + 32x + 57$
137	$y^2 = x^3 + x + 36$	$y^2 = x^3 + 61x + 47$
277	$y^2 = x^3 + 2x + 61$	$y^2 = x^3 + 61x + 47$
311	$y^2 = x^3 + x + 50$	$y^2 = x^3 + 18x + 308$
347	$y^2 = x^3 + 2x + 96$	$y^2 = x^3 + 174x + 12$
467	$y^2 = x^3 + 2x + 361$	$y^2 = x^3 + 234x + 337$
557	$y^2 = x^3 + 3x + 132$	$y^2 = x^3 + 140x + 295$
761	$y^2 = x^3 + x + 82$	$y^2 = x^3 + 592x + 454$
997	$y^2 = x^3 + 6x + 493$	$y^2 = x^3 + 500x + 934$

2.2. Optimal Curves of Genus 2. We start with a proposition which was proved in [8].

Proposition 2.4. *Up to an isomorphism over the field \mathbb{F}_q there exists exactly one maximal (resp. minimal) optimal curve C of genus 2 over \mathbb{F}_q , viz., the fibered product over \mathbb{P}^1 of the two maximal (resp. minimal) optimal elliptic curves*

$$E_1 : y^2 = f(x) \quad \text{and} \quad E_2 : y^2 = f(x)(\alpha x + \beta).$$

Example 2.5. Here we produce examples of elliptic curves E_2 from the proposition above and maximal curve of genus 2 over the finite field \mathbb{F}_q of the discriminant -19 and $q < 1000$.

q	Maximal elliptic curve	Maximal curve of genus two
47	$y^2 = (x^3 + x + 38)(x + 30)$	$z^2 = x^6 + 4x^4 + 22x^2 + 33$
61	$y^2 = (x^3 + 6x + 29)(x + 2)$	$z^2 = x^6 + 55x^4 + 18x^2 + 9$
137	$y^2 = (x^3 + x + 36)(x + 18)$	$z^2 = x^6 + 83x^4 + 14x^2 + 77$
277	$y^2 = (x^3 + 2x + 61)(2x + 80)$	$z^2 = 104x^6 + 247x^4 + 185x^2 + 245$
311	$y^2 = (x^3 + x + 50)(x + 134)$	$z^2 = x^6 + 220x^4 + 66x^2 + 19$
347	$y^2 = (x^3 + 2x + 96)(x + 166)$	$z^2 = x^6 + 196x^4 + 84x^2 + 316$
467	$y^2 = (x^3 + 2x + 361)(x + 47)$	$z^2 = x^6 + 326x^4 + 91x^2 + 118$
557	$y^2 = (x^3 + 3x + 132)(2x + 266)$	$z^2 = 209x^6 + 318x^4 + 356x^2 + 421$
761	$y^2 = (x^3 + 3x + 132)(x + 257)$	$z^2 = x^6 + 751x^4 + 288x^2 + 98$
997	$y^2 = (x^3 + 3x + 132)(x + 760)$	$z^2 = x^6 + 711x^4 + 20x^2 + 30$

Note that the corresponding minimal curves of genus 2 can be obtained by twisting of maximal curves.

3. A DEGREE OF A PROJECTION

We can calculate the degree of the maps $C \rightarrow E$, obtained via the embedding of C into $\text{Jac}(C) \cong E^g$ and projections onto E .

The following result can be found in [8], we include it here with the proof for the sake of completeness. Note that proof relies on the fact that the hermitian lattice corresponding to $\text{Jac}(C)$ is a free \mathcal{O}_K -module, which holds in the case when \mathbb{F}_q has discriminant -19 .

Proposition 3.1. *Let C be an optimal curve over \mathbb{F}_q . Fix an isomorphism $\text{Jac}(C) \cong E^g$ such that the theta divisor corresponds to the hermitian form (h_{ij}) on \mathcal{O}_K^g on the canonical lift of $\text{Jac}(C)$. Then degree of the k -th projection*

$$f_k : C \hookrightarrow \text{Jac}(C) \cong E^g \xrightarrow{\text{pr}_k} E$$

equals $\det(h_{ij})_{i,j \neq k}$.

Proof. We enumerate factors of the abelian variety E^g by $E_1 \times \dots \times E_g$, where $E_i = E$, and consider the first projection. The degree of the map f_1 equals the intersection number $[C] \cdot [E_2 \times \dots \times E_g]$. The cohomology class $[C]$ of C in an appropriate cohomology theory is $[\Theta^{g-1}/(g-1)!]$. Recall that if L is a line bundle on an abelian variety A of dimension g then by the Riemann-Roch theorem one has $(L^g/g!)^2 = \deg(\varphi_L)$, and $\deg(\varphi_L) = \det(r_{ij})^2$, where the matrix (r_{ij}) gives the hermitian form corresponding to the first Chern class of the line bundle L . Since the hermitian form $(h_{ij})_{i,j \neq 1}$ corresponds to the line bundle $\Theta|_{E_2 \times \dots \times E_g}$ on the abelian variety $E_2 \times \dots \times E_g$ the degree of f_1 is given by

$$[C] \cdot [E_2 \times \dots \times E_g] = \frac{1}{(g-1)!} (\Theta|_{E_2 \times \dots \times E_g})^{g-1} = \det((h_{ij})_{i,j \neq 1}).$$

□

4. PROPERTIES OF THE AUTOMORPHISM GROUP

In this section we prove that an optimal curve of genus 3 over a finite field with the discriminant is -19 is not hyperelliptic. Furthermore, we prove that there exists either a maximal or a minimal curve.

From the table of classification of hermitian modules with discriminant -19 along with the Lemma 4.2 proved that an order of an automorphism group of an optimal curve of genus 3 over a finite field with the discriminant -19 is 6.

Proposition 4.1. *There exists an optimal curve C of genus 3 over \mathbb{F}_q , namely the double covering of a maximal or minimal elliptic curve respectively.*

Proof. The equivalence of categories as described in the Introduction tells us that a polarization of the Jacobian corresponds to a class of irreducible unimodular hermitian forms. According to the classification [5] of unimodular hermitian modules, there is a unique class of irreducible unimodular hermitian forms. This class can be represented by the unimodular hermitian matrix below.

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & \frac{-3+\sqrt{-19}}{2} \\ -1 & \frac{-3-\sqrt{-19}}{2} & 3 \end{pmatrix}.$$

Therefore by the Theorem of Oort and Ueno [4], there exists a unique \mathbb{F}_q -isomorphism class of optimal curves over \mathbb{F}_q . By Proposition 3.1 the degree of $f_1 : C \rightarrow E$ is equal to the determinant

$$\det \begin{pmatrix} 3 & \frac{-3+\sqrt{-19}}{2} \\ \frac{-3-\sqrt{-19}}{2} & 3 \end{pmatrix}$$

which is 2. Hence C is a double covering of an optimal elliptic curve, as desired. \square

Now we show an optimal curve of genus 3 is not hyperelliptic.

Lemma 4.2. *Let C be an optimal curve of genus 3 over a finite field \mathbb{F}_q with discriminant -19 . Then C is non-hyperelliptic.*

Proof. For the sake of contradiction suppose that C is a hyperelliptic curve. Then there are two involutions, the first involution τ is the hyperelliptic involution and the second involution σ corresponds to the double cover $f_1 : C \rightarrow E$ from the previous proposition. So $C/\langle\sigma\rangle$ is an optimal elliptic curve and $C/\langle\tau\rangle$ is a projective line. The subgroup $\langle\sigma, \tau\rangle$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and we have the following diagram of coverings

$$\begin{array}{ccccc} & & C & & \\ & \swarrow 2:1 & \downarrow 2:1 & \searrow 2:1 & \\ C/\langle\sigma\rangle \cong E & & C/\langle\sigma\tau\rangle & & \mathbb{P}^1 \\ & \searrow 2:1 & \downarrow 2:1 & \swarrow 2:1 & \\ & & \mathbb{P}^1 & & \end{array}$$

Furthermore the formal relation of groups

$$2 \cdot \frac{1}{4} \{id, \tau, \sigma, \sigma\tau\} + \{id\} = \frac{1}{2} \{id, \sigma\} + \frac{1}{2} \{id, \tau\} + \frac{1}{2} \{id, \sigma\tau\}$$

implies the relation between idempotents in $\text{End}(\text{Jac}(C))$ (see [2]) and therefore we have an isogeny

$$(4.1) \quad \text{Jac}(C) \sim \text{Jac}(C/\langle\sigma\rangle) \times \text{Jac}(C\langle\sigma \circ \tau\rangle).$$

From the isogeny above and Hurwitz' formula, it follows that $C \rightarrow C/\langle\sigma\rangle$ is an unramified double covering. Therefore the number of rational points $\#C(\mathbb{F}_q)$ is even. On other hand $\#C(\mathbb{F}_q) = q + 1 \pm 3m$ is odd since m is odd. \square

The next lemma shows the relation between minimal and maximal curves.

Lemma 4.3. *Let \mathbb{F}_q be a finite field with discriminant -19 . Then \mathbb{F}_q cannot admit minimal and maximal curves simultaneously.*

Proof. Suppose there exist a maximal curve C_M and a minimal curve C_m over \mathbb{F}_q . Then $\text{Jac}(C_M \times_{\mathbb{F}_q} \mathbb{F}_{q^2}) \cong \text{Jac}(C_m \times_{\mathbb{F}_q} \mathbb{F}_{q^2})$ and hence we have an \mathbb{F}_{q^2} -isomorphism $(C_M \times_{\mathbb{F}_q} \mathbb{F}_{q^2}) \cong (C_m \times_{\mathbb{F}_q} \mathbb{F}_{q^2})$.

We denote $C_M \times_{\mathbb{F}_q} \mathbb{F}_{q^2}$ by C . Then there are automorphisms F_M and F_m on C which are induced by corresponding Frobenius endomorphisms. In other words if $\mathbb{F}_q(C_M) \cong \mathbb{F}_q(x, y)$ and $\mathbb{F}_q(C_m) \cong \mathbb{F}_q(u, w) \subset \mathbb{F}_{q^2}(C)$ then $\mathbb{F}_{q^2}(C) = \mathbb{F}_q(x, y)$,

$$F_M : \begin{cases} \mathbb{F}_{q^2}(C) \longrightarrow \mathbb{F}_{q^2}(C) \\ \frac{\sum \alpha_{ij} x^i y^j}{\sum \beta_{lm} x^l y^m} \longmapsto \frac{\sum \alpha_{ij}^q x^i y^j}{\sum \beta_{lm}^q x^l y^m}, \end{cases}$$

and

$$F_m : \begin{cases} \mathbb{F}_{q^2}(C) = \mathbb{F}_{q^2}(u, w) \longrightarrow \mathbb{F}_{q^2}(u, w) \\ \frac{\sum \alpha_{ij} u^i w^j}{\sum \beta_{lm} u^l w^m} \longmapsto \frac{\sum \alpha_{ij}^q u^i w^j}{\sum \beta_{lm}^q u^l w^m}, \end{cases}$$

From the construction of the automorphisms F_M, F_m it follows that the quotient curves $C/\langle F_M \rangle$ and $C/\langle F_m \rangle$ are defined over \mathbb{F}_q and

$$\mathbb{F}_q(C/\langle F_M \rangle) = \mathbb{F}_{q^2}(C)^{\langle F_M \rangle} = \mathbb{F}_q(C_M),$$

$$\mathbb{F}_q(C/\langle F_m \rangle) = \mathbb{F}_{q^2}(C)^{\langle F_m \rangle} = \mathbb{F}_q(C_m).$$

The automorphisms F_m and F_M induce automorphisms on $\text{Jac}(C)$ which we, by abuse of notation, denote by F_m and F_M , respectively. In $\text{End}_{\mathbb{F}_{q^2}}(\text{Jac}(C))$ we have the relation $F_m^2 = F_M^2$ and hence $F_m = -F_M$, since the two are distinct. On the other hand the automorphism F_m and F_M induce two different automorphisms of C . Therefore by Torelli's Theorem C must be a hyperelliptic curve. But we showed that this is impossible in Lemma 4.2. \square

5. EQUATIONS OF OPTIMAL CURVES OF GENUS 3

In this section we combine the theoretical results which we derived in order to produce optimal curves of genus 3 over finite fields with discriminant -19 .

Theorem 5.1. *Let C be an optimal curve over \mathbb{F}_q . Then C can be written in one of the following forms:*

$$\begin{cases} z^2 = \alpha_0 + \alpha_1x + \alpha_2x^2 + \beta_0y, \\ y^2 = x^3 + ax + b, \end{cases}$$

$$\begin{cases} z^2 = \alpha_0 + \alpha_1x + \alpha_2x^2 + (\beta_0 + \beta_1x)y, \\ y^2 = x^3 + ax + b, \end{cases}$$

$$\begin{cases} z^2 = \alpha_0 + \alpha_1x + \alpha_2x^2 + \alpha_3x^3 + (\beta_0 + \beta_1x)y, \\ y^2 = x^3 + ax + b, \end{cases}$$

with coefficients in \mathbb{F}_q and the equation $y^2 = x^3 + ax + b$ corresponding to an optimal elliptic curve.

Proof. Let C be an optimal curve of genus 3 over a finite field \mathbb{F}_q and let $f : C \rightarrow E$ be a double covering of C with the equation $y^2 = x^3 + ax + b$. Set $D = f^{-1}(\infty') = \sum_{P|\infty'} e(P|\infty') \cdot P \in \text{Div}(C)$, where $\infty' \in E$ lies over $\infty \in \mathbb{P}^1$ by the action $E \rightarrow \mathbb{P}^1$, $\deg D = 2$.

By Riemann-Roch Theorem

$$\dim D = \deg D + 1 - g + \dim(W - D) = \dim(W - D),$$

where W is a canonical divisor of the curve C . Consequently, D is equivalent to the positive divisor $W - D_1$, where $\deg D_1 = 2$. Conclude $\dim D = \dim(W - D) < \dim W = 3$. Taking into account that C is a non-hyperelliptic curve and $\deg D = 2$, we conclude $\dim D = 1$.

Consider the divisor $2D$. By Clifford's Theorem

$$\dim 2D \leq 1 + \frac{1}{2} \deg 2D.$$

Therefore, $\dim 2D \leq 3$.

We separate the proof into three cases.

(1) Suppose $\dim 2D = 3$.

Then there exist linearly independent elements $1, x, z' \in L(2D)$. Seven elements $1, x, x^2, y, z', (z')^2, zx$ lie in the vector space $L(4D)$. Since $\dim 4D = 6$, then there exists relation

$$a_1 z'^2 + a_2 z' + a_3 z'x = a_4 + a_5x + a_6x^2 + a_7y,$$

where $a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{F}_q$. Recall that $a_1 \neq 0$, otherwise the equation for z' over $k(x, y)$ will be of degree 1, which is a contradiction, since $[k(C) : k(x, y)] = 2$. Dividing both parts of the equation by a_1 and making the substitution $z = z' + (\frac{a_2}{a_1} + \frac{a_3}{a_1}x)/2$, we obtain the equation

$$z^2 = \alpha_0 + \alpha_1x + \alpha_2x^2 + \beta_0y.$$

- (2) Suppose $\dim(2D) = 2$ and $D = Q_1 + Q_2$, where $Q_1 \neq Q_2$, $Q_1, Q_2 \in C(\mathbb{F}_q)$.

Then we have $\dim(2D + Q_1) = 3$, by Riemann-Roch Theorem. The elements $1, x, x^2, y, z, z^2, xz, yz, xz^2 \in L(4D + 2Q_1)$ are linearly dependent since $\dim(4D + 2Q_1) = 8$ and $x \in L(2D)$, $z \in L(2D + Q_1)$, $y \in L(3D)$. Therefore,

$$z^2(\alpha_0 + \alpha_1x) + z(\beta_0 + \beta_1x + \beta_2y) + (\gamma_0 + \gamma_1x + \gamma_2x^2 + \delta y) = 0.$$

Denoting the expressions in brackets by $\varphi_1, \varphi_2, \varphi_3$ respectively, we rewrite the expression above as

$$z^2\varphi_1 + z\varphi_2 + \varphi_3 = 0.$$

Knowing that $\varphi_1 = \alpha_0 + \alpha_1x \neq 0$ (otherwise $v_{P_1}(x) = 0$) and the equation above can be rewritten as

$$(z + \frac{\varphi_2}{2\varphi_1})^2 + \frac{\varphi_3}{\varphi_1} - \frac{\varphi_2^2}{4\varphi_1^2} = 0.$$

After appropriate substitutions we get the desired equation

$$z^2 = \alpha_0 + \alpha_1x + \alpha_2x^2 + \alpha_3x^3 + (\beta_0 + \beta_1x)y.$$

- (3) Suppose $\dim(2D) = 2$ and $D = Q_1 + Q_2 = 2Q$, where $Q_1 = Q_2 = Q \in C(\mathbb{F}_q)$.

In order to manage this case we prove that the elements $1, x, z, y, x^2, z^2, xy, xz$ are linearly dependent. As a corollary of this fact we obtain the equation of the second type.

In this case the functions $x \in L(2D)$, $y \in L(3D)$ have pole divisors $(x)_\infty = 4Q$, $(y)_\infty = 6Q$, and there is a function $z \in L(2D + Q)$ such that $(z)_\infty = 5Q$.

The element z is an integral element over $\mathbb{F}_q[x, y]$. Indeed, either

$$1, x, z, y, x^2, z^2, xy, xz \in L(10D)$$

or

$$1, x, y, z, x^2, zx, xy, z^2, zy, x^3, zx^2, xyz, z^3 \in L(15Q)$$

are linearly dependent and in both cases we have relations with nonzero leading coefficients at z . This yields that z is integral over $\mathbb{F}_q[x, y]$.

It is clear that $z \notin \mathbb{F}_q(x, y)$ (otherwise 2 divides $v_Q(z) = 5$).

The minimal polynomial of z has degree 2 and coefficients in $\mathbb{F}_q[x, y]$, since the degree of extension $[\mathbb{F}_q(C) : \mathbb{F}_q(x, y)]$ is 2. Therefore we have that

$$z^2 + \sum_{i \geq 0} a_i z y x^i + \sum_{j \geq 0} b_j z x^j + \sum_{l \geq 0} c_l x^l + \sum_{s \geq 0} d_s y x^s = 0,$$

and hence

$$(5.1) \quad \begin{aligned} & z^2 + c_0 + c_1 x + c_2 x^2 + d_0 y + b_0 z + b_1 z x + d_1 x y = \\ & = -z(b_2 x^2 + \dots) + z y(a_0 + a_1 x + \dots) + (c_4 x^4 + \dots) + y(d_2 x^2 + \dots). \end{aligned}$$

Furthermore, we have

- $v_Q(z x^i) = -5 - 4i \equiv 3 \pmod{4}$
- $v_Q(z y x^j) = -5 - 6 - 4i \equiv 1 \pmod{4}$
- $v_Q(x^l) = -4l \equiv 0 \pmod{4}$
- $v_Q(y x^i) = -6 - 4i \equiv 2 \pmod{4}$.

If the right part of the equation 5.1 is non-zero, then we can apply the strict triangle inequality. As a consequence we get that on the one hand

$$v_Q(z^2 + c_0 + c_1 x + c_2 x^2 + d_0 y + b_0 z + b_1 z x + d_1 x y) \leq -11$$

and on the other hand

$$v_Q(z^2 + c_0 + c_1 x + c_2 x^2 + d_0 y + b_0 z + b_1 z x + d_1 x y) \geq -10.$$

Therefore the right part of the equation above is zero, i. e. the elements $1, x, z, y, x^2, z^2, xy, xz$ are linearly dependent.

□

Example 5.2. We produce examples of optimal curves over finite fields with discriminant -19 . It suffices to find either a maximal or a minimal curve as their existence is mutually exclusive.

q	Maximal optimal curve	Minimal optimal curve
47	$y^2 = x^3 + x + 38,$ $z^2 = 10x^2 + 46x + 39 + y$	-
61	$y^2 = x^3 + 6x + 29,$ $z^2 = x^2 + 54x + 38 + 3y$	-
137	$y^2 = x^3 + x + 36,$ $z^2 = 3x^2 + 95x + 92 + 10y$	-
277	$y^2 = x^3 + 2x + 61,$ $z^2 = x^2 + 33x + 212 + 5y$	-
311	$y^2 = x^3 + 18x + 308,$ $z^2 = 11x^2 + 222x + 32 + 65y$	-
347	-	$y^2 = x^3 + 174x + 12,$ $z^2 = 2x^2 + 310x + 219 + 94y$
467	$y^2 = x^3 + 2x + 361,$ $z^2 = 2x^2 + 381x + 242 + 159y$	-
557	-	$4y^2 = x^3 + 2x + 151,$ $z^2 = 439 + 322x + 5x^2 + 122y$
761	$y^2 = x^3 + 4x + 105,$ $z^2 = 406 + 131x + 3x^2 + 247y$	-
997	-	$y^2 = x^3 + 500x + 934,$ $z^2 = x^2 + 336x + 564 + 196y$

REFERENCES

- [1] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.*, 8:238–243, 1969.
- [2] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.
- [3] Kristin Lauter. The maximum or minimum number of rational points on genus three curves over finite fields. *Compositio Math.*, 134(1):87–111, 2002. With an appendix by Jean-Pierre Serre.
- [4] Frans Oort and Kenji Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:377–381, 1973.
- [5] Alexander Schiemann. Classification of Hermitian forms with the neighbour method. *J. Symbolic Comput.*, 26(4):487–508, 1998.
- [6] Gerard van der Geer and Marcel van der Vlugt. Supersingular curves of genus 2 over finite fields of characteristic 2. *Math. Nachr.*, 159:73–81, 1992.
- [7] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.
- [8] A. Zaytsev. Optimal curves of low genus over finite fields, 2007. <http://arxiv.org/abs/0706.4203>.

E. ALEKSEENKO , S. ALESHNIKOV, IMMANUEL KANT STATE UNIVERSITY OF RUSSIA, NEVSKY 14, KALININGRAD, RUSSIA

N. MARKIN, A. ZAYTSEV, SCHOOL OF MATHEMATICAL SCIENCES,
UCD CASL, BELFIELD OFFICE PARK, DUBLIN 4

E-mail address: alexey.zaytsev@ucd.ie